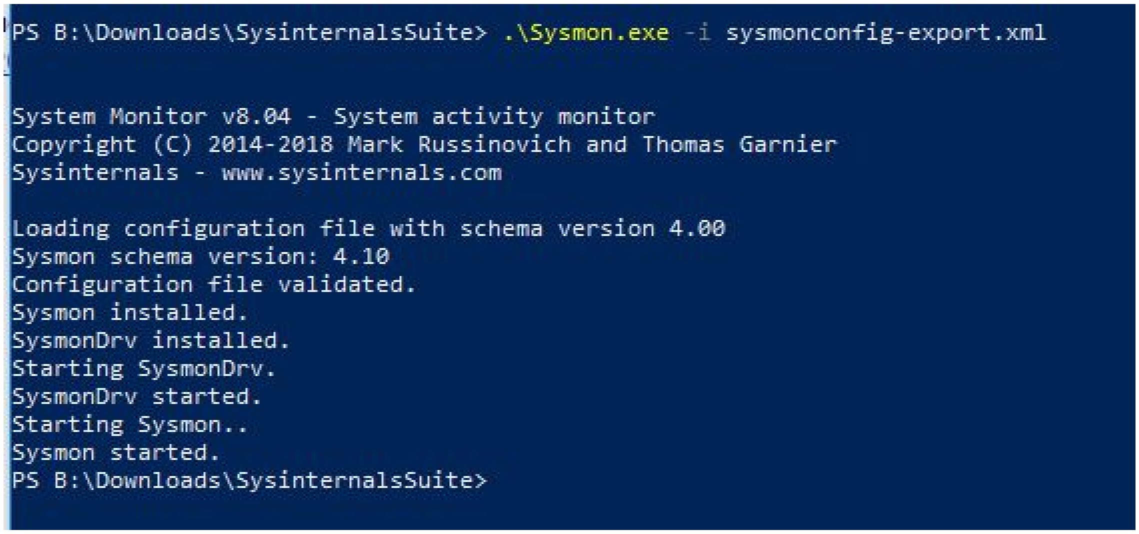
Sysmon

- **Install and extract SysInternals Suite from Microsoft:**
    - https://docs.microsoft.com/en-us/sysinternals/downloads/
- **Download the config file from github**
    - https://github.com/SwiftOnSecurity/sysmon-config
    - Make sure the config file is in the same folder as Sysmon
- **Run Sysmon**
    - .\sysmon.exe -i sysmonconfig-export.xml

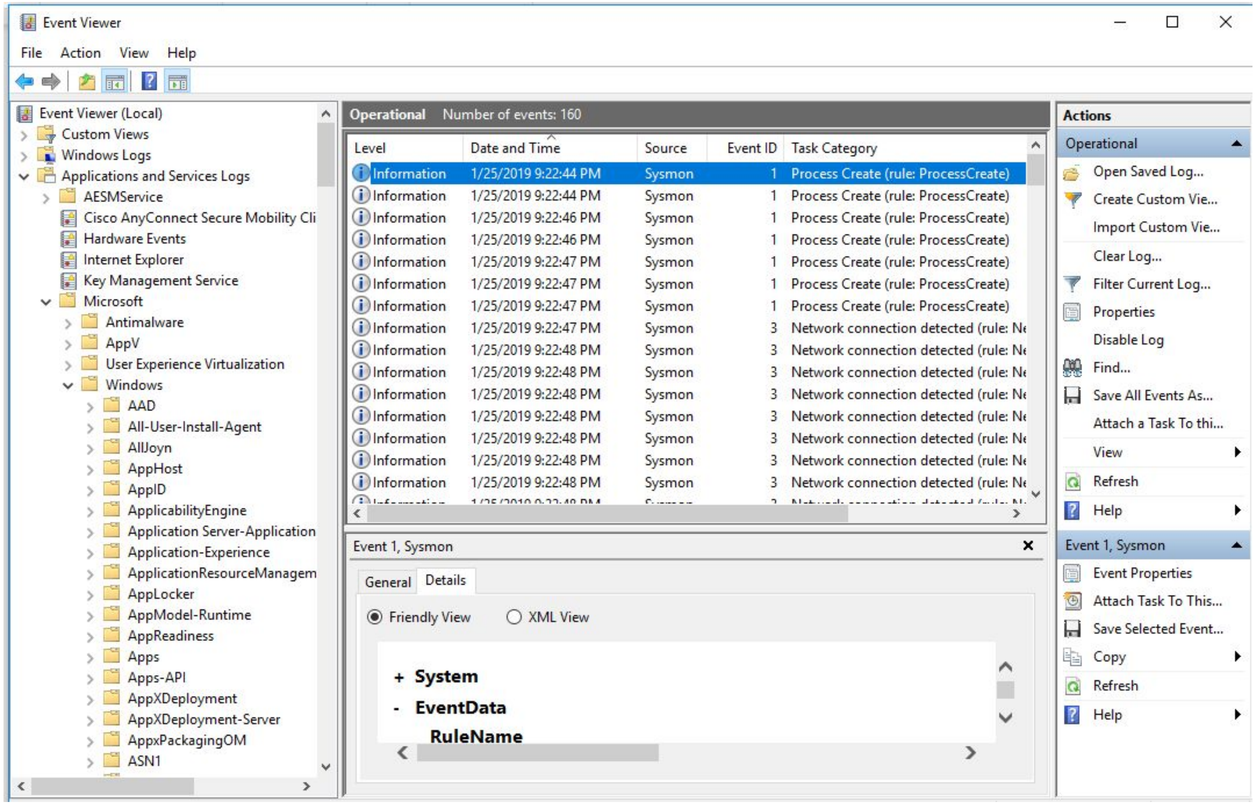


```
PS B:\Downloads\SysinternalsSuite> .\Sysmon.exe -i sysmonconfig-export.xml


System Monitor v8.04 - System activity monitor
Copyright (C) 2014-2018 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.00
Sysmon schema version: 4.10
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
PS B:\Downloads\SysinternalsSuite>
```

- **Open Event Viewer**
    - “Control Panel/Administrative Tools/Event Viewer/Applications and Services Logs/Microsoft/Windows/Sysmon/Operational”



Operational Number of events: 160

Level	Date and Time	Source	Event ID	Task Category
Information	1/25/2019 9:22:44 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	1/25/2019 9:22:44 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	1/25/2019 9:22:46 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	1/25/2019 9:22:46 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	1/25/2019 9:22:47 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	1/25/2019 9:22:47 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	1/25/2019 9:22:47 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	1/25/2019 9:22:47 PM	Sysmon	3	Network connection detected (rule: Ne
Information	1/25/2019 9:22:48 PM	Sysmon	3	Network connection detected (rule: Ne
Information	1/25/2019 9:22:48 PM	Sysmon	3	Network connection detected (rule: Ne
Information	1/25/2019 9:22:48 PM	Sysmon	3	Network connection detected (rule: Ne
Information	1/25/2019 9:22:48 PM	Sysmon	3	Network connection detected (rule: Ne
Information	1/25/2019 9:22:48 PM	Sysmon	3	Network connection detected (rule: Ne
Information	1/25/2019 9:22:48 PM	Sysmon	3	Network connection detected (rule: Ne
Information	1/25/2019 9:22:48 PM	Sysmon	3	Network connection detected (rule: Ne

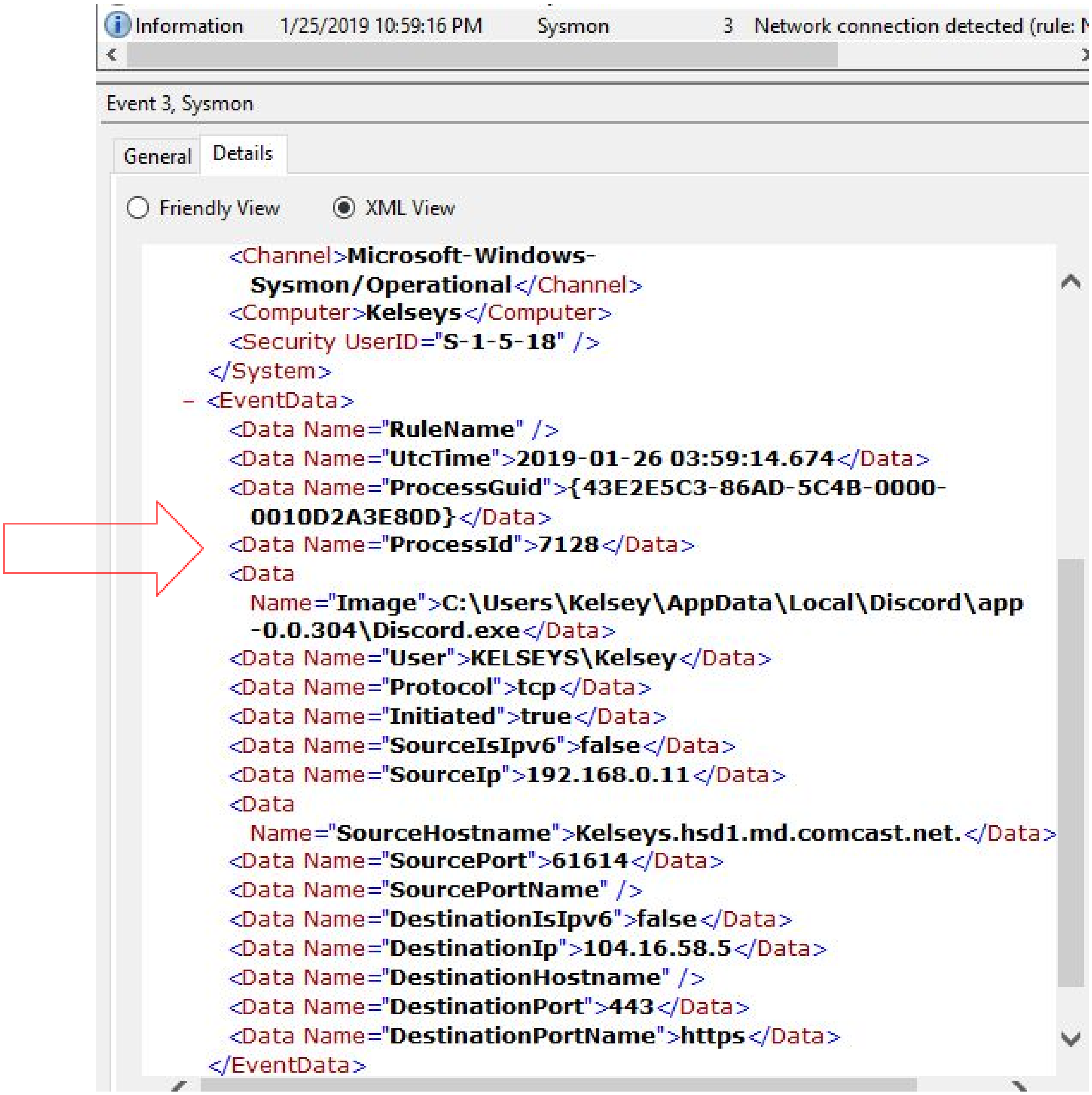
Event 1, Sysmon

General Details

● Friendly View ○ XML View

+ System
- EventData
RuleName

- **View more information on a selected event**
  - **Find its PID (Process ID)**



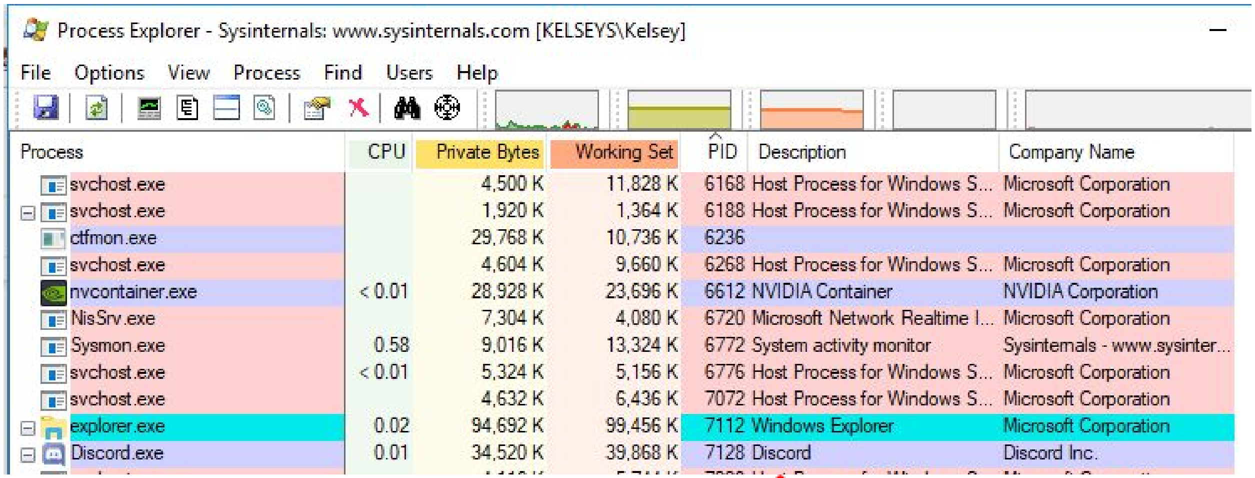
Information 1/25/2019 10:59:16 PM Sysmon 3 Network connection detected (rule: N

Event 3, Sysmon

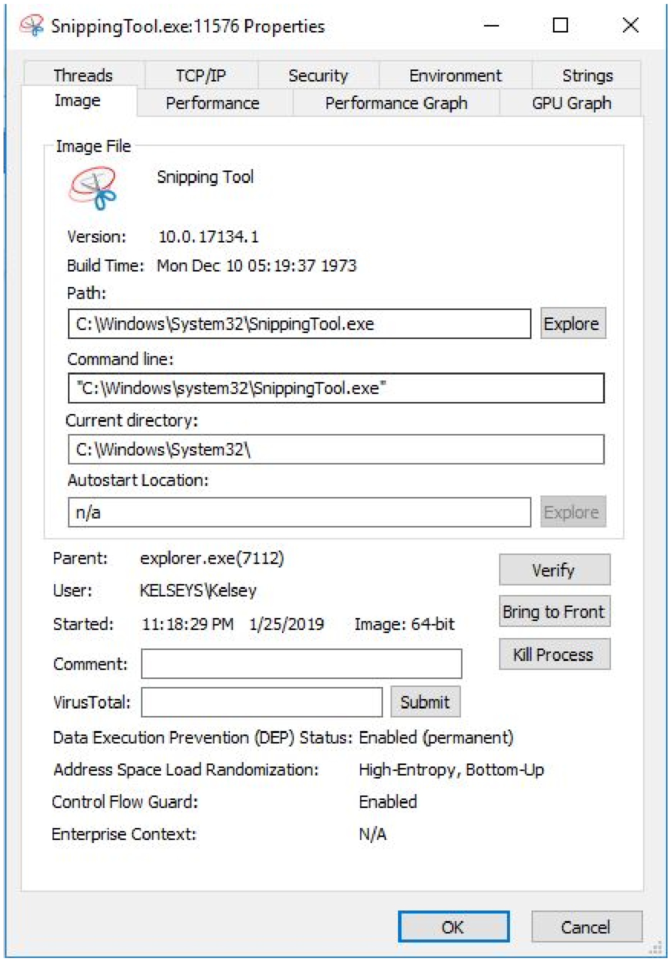
○ Friendly View ● XML View

```
    <Channel>Microsoft-Windows-
      Sysmon/Operational</Channel>
    <Computer>Kelseys</Computer>
    <Security UserID="S-1-5-18" />
  </System>
- <EventData>
    <Data Name="RuleName" />
    <Data Name="UtcTime">2019-01-26 03:59:14.674</Data>
    <Data Name="ProcessGuid">{43E2E5C3-86AD-5C4B-0000-
      0010D2A3E80D}</Data>
    <Data Name="ProcessId">7128</Data>
    <Data
      Name="Image">C:\Users\Kelsey\AppData\Local\Discord\app
      -0.0.304\Discord.exe</Data>
    <Data Name="User">KELSEYS\Kelsey</Data>
    <Data Name="Protocol">tcp</Data>
    <Data Name="Initiated">true</Data>
    <Data Name="SourceIsIpv6">false</Data>
    <Data Name="SourceIp">192.168.0.11</Data>
    <Data
      Name="SourceHostname">Kelseys.hsd1.md.comcast.net.</Data>
    <Data Name="SourcePort">61614</Data>
    <Data Name="SourcePortName" />
    <Data Name="DestinationIsIpv6">false</Data>
    <Data Name="DestinationIp">104.16.58.5</Data>
    <Data Name="DestinationHostname" />
    <Data Name="DestinationPort">443</Data>
    <Data Name="DestinationPortName">https</Data>
  </EventData>
```

- **Find the PID in Process Explorer**
  - Procexp is found in the Sysinternals Suite
  - Sorting by PID makes it easier to find


Process Explorer - Sysinternals: www.sysinternals.com [KELSEYS\Kelsey]
File
Options
View
Process
Find
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		4,500 K	11,828 K	6168	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,920 K	1,364 K	6188	Host Process for Windows S...	Microsoft Corporation
ctfmon.exe		29,768 K	10,736 K	6236		
svchost.exe		4,604 K	9,660 K	6268	Host Process for Windows S...	Microsoft Corporation
nvcontainer.exe	< 0.01	28,928 K	23,696 K	6612	NVIDIA Container	NVIDIA Corporation
NisSrv.exe		7,304 K	4,080 K	6720	Microsoft Network Realtime I...	Microsoft Corporation
Sysmon.exe	0.58	9,016 K	13,324 K	6772	System activity monitor	Sysinternals - www.sysinter...
svchost.exe	< 0.01	5,324 K	5,156 K	6776	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,632 K	6,436 K	7072	Host Process for Windows S...	Microsoft Corporation
explorer.exe	0.02	94,692 K	99,456 K	7112	Windows Explorer	Microsoft Corporation
Discord.exe	0.01	34,520 K	39,868 K	7128	Discord	Discord Inc.



Snipping Tool

Version: 10.0.17134.1

Build Time: Mon Dec 10 05:19:37 1973

Path: C:\Windows\System32\SnippingTool.exe

Command line: "C:\Windows\system32\SnippingTool.exe"

Current directory: C:\Windows\System32\

Autostart Location: n/a

Parent: explorer.exe(7112)

User: KELSEYS\Kelsey

Started: 11:18:29 PM 1/25/2019 Image: 64-bit

Comment:

VirusTotal:

Data Execution Prevention (DEP) Status: Enabled (permanent)

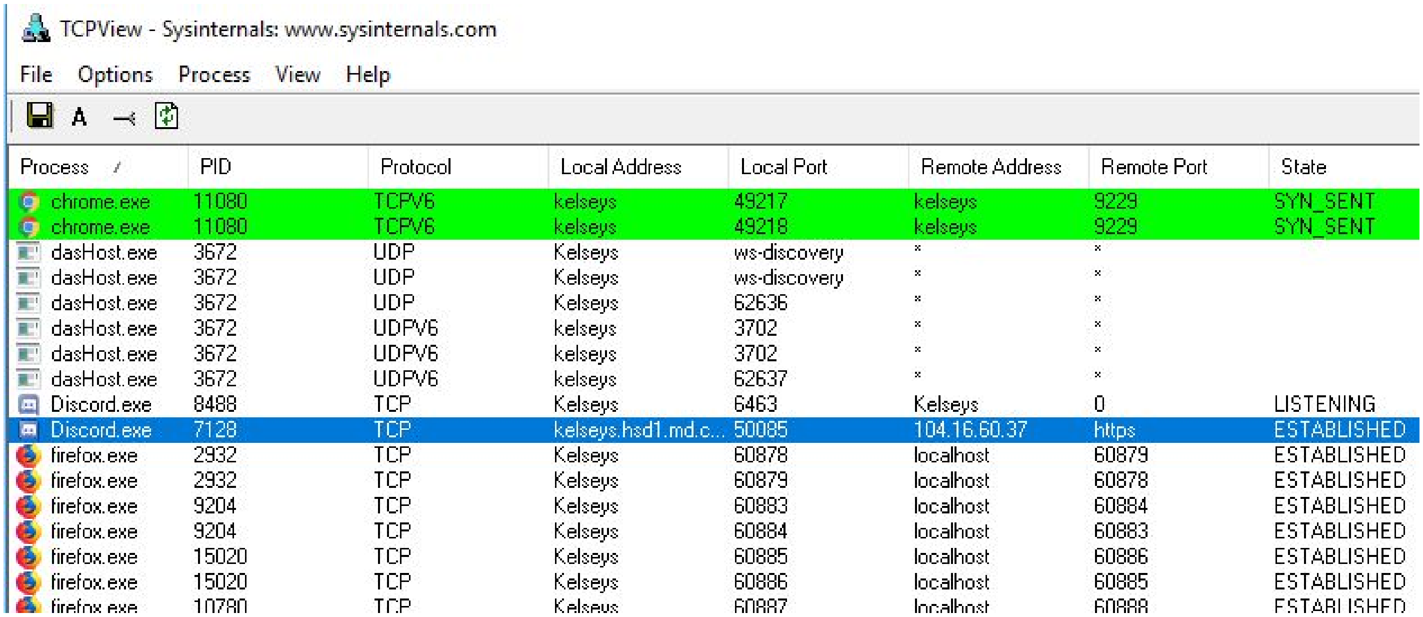
Address Space Load Randomization: High-Entropy, Bottom-Up

Control Flow Guard: Enabled

Enterprise Context: N/A

- Double clicking on a process displays its properties, such as the parent process and the user who created the process

- **Find Information on a Network Connection via TCPView**
    - **If the event viewed in Event viewer was an Event ID 3, it is a network connection**
    - **Find the connection’s PID via Event viewer and open TCPView (from Sysinternals Suite)**
    - **Press space to pause refreshes in TCPView**
    - **Find the PID and view its information**



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
chrome.exe	11080	TCPV6	kelseys	49217	kelseys	9229	SYN_SENT
chrome.exe	11080	TCPV6	kelseys	49218	kelseys	9229	SYN_SENT
dasHost.exe	3672	UDP	Kelseys	ws-discovery	*	*	
dasHost.exe	3672	UDP	Kelseys	ws-discovery	*	*	
dasHost.exe	3672	UDP	Kelseys	62636	*	*	
dasHost.exe	3672	UDPV6	kelseys	3702	*	*	
dasHost.exe	3672	UDPV6	kelseys	3702	*	*	
dasHost.exe	3672	UDPV6	kelseys	62637	*	*	
Discord.exe	8488	TCP	Kelseys	6463	Kelseys	0	LISTENING
Discord.exe	7128	TCP	kelseys.hsd1.md.c...	50085	104.16.60.37	https	ESTABLISHED
firefox.exe	2932	TCP	Kelseys	60878	localhost	60879	ESTABLISHED
firefox.exe	2932	TCP	Kelseys	60879	localhost	60878	ESTABLISHED
firefox.exe	9204	TCP	Kelseys	60883	localhost	60884	ESTABLISHED
firefox.exe	9204	TCP	Kelseys	60884	localhost	60883	ESTABLISHED
firefox.exe	15020	TCP	Kelseys	60885	localhost	60886	ESTABLISHED
firefox.exe	15020	TCP	Kelseys	60886	localhost	60885	ESTABLISHED
firefox.exe	10780	TCP	Kelseys	60887	localhost	60888	ESTABLISHED